**IT Applications, Ch 7, Information Management**

**Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.**

**Complete the following from p 270-**

**Deliberate threats**

1. **When does intentional damage occur?**

Intentional damage occurs when an individual or group deliberately sets out to cause problems within an information system.

1. **Unauthorised access is both physical and logical. Explain what this means?**

The physical part refers to stealing or breaking equipment, whereas gaining access to confidential files on a restricted site via the internet connection is considered a logical breach.

1. **Computer Virus**
   1. **Describe the nature of this virus.**

A virus may prevent the normal use of the computer and can even destroy data or the hardware.

* 1. **What is the main purpose of a virus?**

Computer viruses are programs written with the intention of disrupting normal computer operation or destroying data or hardware.

* 1. **What is meant by the term, payload?**

The payload is the destructive part of the virus. It is the action that the virus is designed to carry out, such as deleting files from the heard dick or randomly sending emails to recipients found in the address book.

* 1. **Describe a worm?**

A worm is a virus that self-replicates to take up space on the hard drive on a single work station or server.

* 1. **List the other types of viruses, p 272, fig. 7-10.**
* Boot infections
* Executable
* Macro
* Time bomb
* Logic bomb
* Worm
* Trojan horse
* Resident
* Polymorphic
  1. **How do viruses mainly spread?**

The most common way that viruses spread is via email attachment or by the transition of infected files on removable storage devices

1. **Hacking/Cracking**
   1. **Who is a hacker and what damage do they cause?**

A hacker is a person that gains unauthorised access to an information system through logical means in order to look at the stored data or simply for the challenge. A hacker may use the information found to blackmail the organisation; crackers are more associated with the destroying, altering or stealing of data, which can be more harmful.

1. **Tampering with files**
   1. **Describe how employees tamper with files.**

Employee may tamper with files in order to change information to suit their liking, for example, change salary amounts.

* 1. **What is industrial sabotage?**

Industrial sabotage istampering but on a larger scale, related to the whole organisation. Most times competitors will perform industrial sabotage in order for that organisation to loos profits or become weaker.

1. **Information theft**
   1. **Why does this occur?**

A less competitive organisation may steal information in order to gain a competitive edge and steal ideas and concepts.

1. **Vandalism of hardware**

The vandalism of hardware is the deliberate act of damaging equipment. This may prevent the users from being able to access the information system due to a broken keyboard or mouse, or a broken ticket machine at the train station.

1. **Theft of hardware**

Computer hardware is in great demand and it is popular these days for groups to target organisations and steal smaller items such as digital cameras, RAM chips, external hard drives, laptops and hard disks.

**Accidental threats**

1. **User error**
   1. **List some common examples of user error.**

* Copying older versions of files over new ones.
* Formatting a disk that contains data
* Damaged files due to hardware not being shut down properly.
  1. **What processes are in place to limit user error?**

Must programs try and limit user error by having dialogue boxes to warm of the closing of the program without saving or warnings about deleting files. Most times a program will always request confirmation about an action you are taking.

1. **Failure to follow file-management procedures**
   1. **List common errors of employees in saving files.**

* File extensions have been left off
* Non-descriptive file names were used
* Folders were improperly used.

**Technical Failure**

1. **List some examples of technical failure.**

* CPU, CD drive or graphics card stops working
* Hard disk failure
* Damage from electricity
* Misuse, e.g. dropping a computer.
* Water, smoke, dirt, fire

**Consequences of violating security and privacy measures, p 278**

1. **List three important consequences if security measures are violated.**

* Breaches of security
* Loss of intellectual property
* Loss of income due to availability of information or services